Regenerasi Fungsi $f(x) = x^2 - 7x + 5$ sebagai Pembangkit Bilangan Acak Menggunakan Metode Iterasi Titik Tetap (*Fixed Point Iteration*)

[1]Abednego Irawan , [2]Alz Danny Wowor

Fakultas Teknologi Informasi
Universitas Kristen Satya Wacana
Jl. Dr. O. Notohamidjojo 1-10, Salatiga 50711, Indonesia
Email: [1])672014141@student.uksw.edu, [2])alzdanny.wowor@staff.uksw.edu

Abstract

This study examines whether the quadratic function $f(x) = x^2 - 7x + 5$ can be used as a key generator in cryptography. Sought quadratic function equation using fixed point iteration method and then used as a function of iteration. Taking digit numbers on mantissa to get random numbers (chaos). Tests done by the randomness of observations on cartesian diagram visualization, runs test and correlation test. The function of the equation still shows that it still produces patterned numbers on iteration process. Because it has not been able to produce a chaos line, then the coefficients and constants are manipulated to prove that the quadratic function can produce random number lines with the right selection of coefficients and constants. Based on this research, the manipulation of the coefficients and constants into fractions of an iterative function $x_{i-1} = (0{,}9_{xi-1} - 5)/x_{i-1}$ is usable to be a generate random numbers based on CSPNRG chaos.

Keyword: *Cryptography, Quadratic Function, Key Generator, Fixed Point Iteration Method, Random Numbers.*

Abstrak

Penelitian ini menguji apakah fungsi kuadrat $f(x) = x^2 - 7x + 5$ dapat digunakan sebagai pembangkit kunci dalam kriptografi. Fungsi kuadrat dicari persamaannya dengan menggunakan metode iterasi titik tetap kemudian dijadikan fungsi iterasi. Pengambilan digit angka pada *mantissa* untuk memperoleh bilangan acak. Pengujian keacakan dilakukan dengan melakukan pengamatan pada visualisasi diagram kertesius, uji *runs* dan uji korelasi. Fungsi persamaan masih menunjukkan bahwa tetap menghasilkan bilangan berpola pada proses iterasi. Karena belum dapat menghasilkan baris bilangan acak, maka dilakukan manipulasi nilai koefisien dan konstanta untuk membuktikan bahwa fungsi kuadrat dapat menghasilkan baris bilangan acak dengan pemilihan koefisien dan konstanta yang tepat. Berdasarkan penelitian yang telah dilakukan, manipulasi koefisien dan konstanta menjadi bilangan pecahan dari fungsi iteratif $x_{i-1} = (0{,}9_{xi-1} - 5)/x_{i-1}$ dapat menghasilkan baris bilangan acak berbasis CSPNRG *chaos.*

Kata Kunci: *Kriptografi, Fungsi Kuadrat, Pembangkit Kunci, Metode Iterasi Titik Tetap, Bilangan Acak.*

---

1) Mahasiswa Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana.
2) Staff Pengajar Falkultas Teknologi Informasi, Universitas Kristen Satya Wacana.